







METHOD AND APPARATUS FOR ENCRYPTION HAVING A FEEDBACK REGISTER WITH SELECTABLE TAPS

Patent number: WO9506906
Publication date: 1995-03-09
Inventor: PUHL LARRY C; FINKELSTEIN LOUIS DAVID
Applicant: MOTOROLA INC [US]
Classification:
 - international: G06F1/02
 - european: H03K3/84; H04L9/26
Application number: WO1994US07774 19940711
Priority number(s): US19930114804 19930830

Also published as:

 EP0672273 (A1)
 US5365585 (A1)
 GB2286274 (A)
 FI951946 (A)
 EP0672273 (A4)
 EP0672273 (B1)

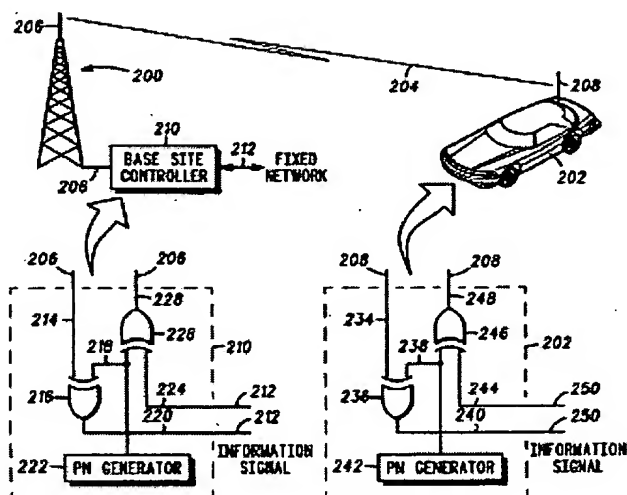
less <<

Cited documents:

 US3728533
 US4590601
 US4611183
 US4890252

Abstract of WO9506906

A method and apparatus for generating a pseudo-random bit sequence is provided. A first input bit (260) is determined as a function of bits stored in a shift register (252) in accordance with a first feedback algorithm. In addition, a second input bit (262) is determined as a function of bits stored in the shift register (252) in accordance with a second feedback algorithm. Subsequently, a particular input bit (268) to be provided to the shift register (252) is deterministically selected from the group consisting of the first input bit (260) and the second input bit (262) such that a non-linear pseudo-random sequence may be produced by the shift register (252). In addition, a communication unit which utilizes the pseudo-random bit sequence in encrypting a signal to be transmitted and decrypting a received signal is described.



Data supplied from the esp@cenet database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公表特許公報 (A)

(11) 特許出願公表番号

特表平8-503569

(43) 公表日 平成8年(1996)4月16日

(51) Int.Cl. ⁸	識別記号	庁内整理番号	F I
G 0 6 F 7/58		C 9188-5E	
G 0 9 C 1/00		7259-5J	
H 0 3 K 3/84		Z 9297-5K	
		8842-5J	H 0 4 L 9/00
		7605-5J	H 0 4 B 7/26
			1 0 9 R

審査請求 未請求 予備審査請求 未請求(全 19 頁) 最終頁に続く

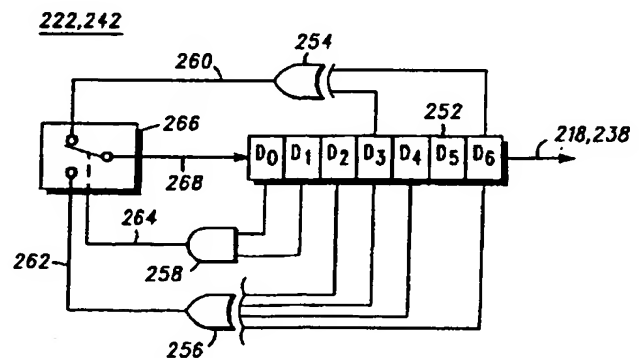
(21) 出願番号 特願平7-508101
(86) (22) 出願日 平成6年(1994)7月11日
(85) 翻訳文提出日 平成7年(1995)4月26日
(86) 国際出願番号 PCT/US94/07774
(87) 国際公開番号 WO95/06906
(87) 国際公開日 平成7年(1995)3月9日
(31) 優先権主張番号 08/114, 804
(32) 優先日 1993年8月30日
(33) 優先権主張国 米国 (US)
(81) 指定国 EP(AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), BR, CA, FI, GB, JP, KR

(71) 出願人 モトローラ・インコーポレイテッド
アメリカ合衆国イリノイ州60196シャンパ
ーグ、イースト・アルゴンクイン・ロード
1303
(72) 発明者 ブール, ラリー・シー
アメリカ合衆国イリノイ州スリーピー・ホ
ロー、ブラム・コート6
(72) 発明者 ファインケルSTEIN, ルイス・デイビッド
アメリカ合衆国イリノイ州フィーリング、
ウエスト・オタワ・コート1698
(74) 代理人 弁理士 本城 雅則 (外1名)

(54) 【発明の名称】 選択可能なタップを備えたフィードバック・レジスタを有する暗号化装置およびその方法

(57) 【要約】

疑似ランダム・ビット・シーケンスを発生する方法および装置を提供する。第1フィードバック・アルゴリズムにしたがって、シフト・レジスタ(252)に記憶されているビットの関数として、第1入力ビット(260)が決定される。更に、第2フィードバック・アルゴリズムにしたがって、シフト・レジスタ(252)に記憶されているビットの関数として、第2入力ビット(262)が決定される。続いて、前記シフト・レジスタ(252)によって非線形疑似ランダム・シーケンスが生成されるように、前記シフト・レジスタ(252)に供給すべき特定入力ビット(268)が、前記第1入力ビット(260)および第2入力ビット(262)から成る群から決定論的に選択される。更に、前記疑似ランダム・ビット・シーケンスを利用して送信する信号を暗号化すると共に受信信号を復号化する通信装置についても記載する。



【特許請求の範囲】

1. 疑似ランダム・ビット・シーケンス発生器であって；

（a）所定数のビットを記憶するシフト・レジスタ手段；

（b）前記シフト・レジスタ手段に動作可能に結合され、前記シフト・レジスタ手段に記憶されているビットの関数として、第1入力ビットを決定する第1フィードバック手段；

（c）前記シフト・レジスタ手段に動作可能に結合され、前記シフト・レジスタ手段に記憶されているビットの関数として第2入力ビットを決定する第2フィードバック手段；および

（d）前記シフト・レジスタ手段、前記第1フィードバック手段、および前記第2フィードバック手段に動作可能に結合され、前記シフト・レジスタ手段によって非線形疑似ランダム・シーケンスが生成されるように、前記シフト・レジスタ手段に供給すべき特定入力ビットを、前記第1入力ビットおよび前記第2入力ビットから成る群から決定論的に選択する制御手段；

から成ることを特徴とする疑似ランダム・ビット・シーケンス発生器。

2. 前記制御手段は、外部入力に基づくアルゴリズムにしたがって前記特定入力ビットを選択する外部制御機構を含み、前記外部入力は、線形フィードバック・シフト・レジ

スタ出力、クロック初期化信号、およびセルラ・オートマトンから成る群から選択されることを特徴とする請求項1記載の疑似ランダム・ビット・シーケンス発生器。

3. 前記制御手段は、内部入力に基づくアルゴリズムにしたがって前記特定入力ビットを選択する内部制御機構を含み、前記内部入力は、前記シフト・レジスタ手段のパリティ・ビット、前記シフト・レジスタ手段の複数のビットの関数、および前記シフト・レジスタ手段の複数の抜き取られていないビットの関数から成る群から選択されることを特徴とする請求項1記載の疑似ランダム・ビット・シーケンス発生器。

4. 前記制御手段は、それぞれ内部入力および外部入力に基づくアルゴリズムに

したがって前記特定入力ビットを選択する内部および外部制御機構を含むことを特徴とする請求項 1 記載の疑似ランダム・ビット・シーケンス発生器。

5. (a) 前記アルゴリズムは前記内部入力と前記外部入力とを論理的に組み合わせて選択信号を発生することを含み；

(b) 前記内部入力は、前記シフト・レジスタ手段のパリティ・ビット、前記シフト・レジスタ手段の複数のビットの関数、および前記シフト・レジスタ手段の複数の抜き取られていないビットの関数から成る群から選択され；

(c) 前記外部入力は、線形フィードバック・シフト・レジスタ出力、クロック初期化信号、およびセルラ・オート

マトンから成る群から選択される；

ことを特徴とする請求項 4 記載の疑似ランダム・ビット・シーケンス発生器。

6. 前記制御手段は、前記シフト・レジスタ手段の複数のビットによってアドレス指定される参照テーブルから値を選択することから成るアルゴリズムにしたがって、前記特定入力ビットを選択する機構を含むことを特徴とする請求項 1 記載の疑似ランダム・ビット・シーケンス装置。

7. 供給元通信システムの加入者装置と固定ネットワーク通信装置との間で、暗号化プロセスによって機密保持通信を維持するために用いられる通信装置であって；

(a) 非線形疑似ランダム・ビット・シーケンスを発生する疑似ランダム・ビット・シーケンス発生手段であって；

(i) 所定数のビットを記憶するシフト・レジスタ手段；

(ii) 前記シフト・レジスタ手段に動作可能に結合され、前記シフト・レジスタに記憶されているビットの関数として第 1 入力ビットを決定する第 1 フィードバック手段；

(iii) 前記シフト・レジスタ手段に動作可能に結合され、前記シフト・レジスタ手段に記憶されているビットの関数として第 2 入力ビットを決定する第 2 フィードバック手段；および

(iv) 前記シフト・レジスタ手段、前記第 1 フィードバック手段、および前記第

2 フィードバック手段に動作可能に結合され、前記シフト・レジスタ手段に供給すべき特定入力

ビットを、前記第 1 入力ビットおよび前記第 2 入力ビットから成る群から決定論的に選択する制御手段；

から成る前記疑似ランダム・ビット・シーケンス発生手段；

(b) 前記疑似ランダム・ビット・シーケンス発生手段に動作可能に結合され、前記非線形疑似ランダム・ビット・シーケンスの関数として、入力情報信号を暗号化する暗号化手段；および

(c) 前記暗号化手段に動作可能に結合され、前記暗号化された情報信号を通信チャンネルを通じて送信する送信手段；

から成ることを特徴とする通信装置。

8. 供給元通信システムの加入者装置と固定ネットワーク通信装置との間で、暗号化プロセスによって機密保持通信を維持するために用いられる通信装置であって；

(a) 通信チャンネルから暗号化情報信号を受信する受信手段；

(b) 非線形疑似ランダム・ビット・シーケンスを発生する疑似ランダム・ビット・シーケンス発生手段であって；

(i) 所定数のビットを記憶するシフト・レジスタ手段；

(ii) 前記シフト・レジスタ手段に動作可能に結合され、前記シフト・レジスタに記憶されているビットの関数として第 1 入力ビットを決定する第 1 フィードバック手段；

(iii) 前記シフト・レジスタ手段に動作可能に結合され、前記シフト・レジスタ手段に記憶されているビットの関数と

して第 2 入力ビットを決定する第 2 フィードバック手段；および

(iv) 前記シフト・レジスタ手段、前記第 1 フィードバック手段、および前記第 2 フィードバック手段に動作可能に結合され、前記シフト・レジスタ手段に供給すべき特定入力ビットを、前記第 1 入力ビットおよび前記第 2 入力ビットから成

る群から決定論的に選択する制御手段；

から成る前記疑似ランダム・ビット・シーケンス発生手段；

(c) 前記受信手段と前記疑似ランダム・ビット・シーケンス発生手段とに動作可能に結合され、受信した暗号化情報信号を、前記非線形疑似ランダム・ビット・シーケンスの関数として復号化する復号化手段；

から成ることを特徴とする通信装置。

9. 疑似ランダム・ビット・シーケンス発生方法であって；

(a) 第1フィードバック・アルゴリズムにしたがって、シフト・レジスタに記憶されているビットの関数として第1入力ビットを決定する段階；

(b) 第2フィードバック・アルゴリズムにしたがって、前記シフト・レジスタ手段に記憶されているビットの関数として第2入力ビットを決定する段階；および

(c) 前記シフト・レジスタ手段によって非線形疑似ランダム・シーケンスが生成されるように、前記シフト・レジスタ手段に供給すべき特定入力ビットを、前記第1入力ビットおよび前記第2入力ビットから成る群から決定論的に

選択するステップ；

から成ることを特徴とする方法。

10. 前記特定入力ビットを決定論的に選択するステップは；

(a) 線形フィードバック・シフト・レジスタ出力、クロック初期化信号、およびセルラ・オートマトンから成る群から選択される外部入力；

(b) 前記シフト・レジスタのパリティ・ビット、前記シフト・レジスタの複数のビットの関数、および前記シフト・レジスタの複数の抜き取られていないビットの関数から成る群から選択される内部入力；

(c) 前記シフト・レジスタのパリティ・ビット、前記シフト・レジスタの複数のビットの関数、および前記シフト・レジスタの複数の抜き取られていないビットの関数から成る群から選択される内部入力と、線形フィードバック・シフト・レジスタ出力、クロック初期化信号、およびセルラ・オートマトンから成る群から選択される外部入力とを、論理的に組み合わせることによって得られる選択信

号；および

(d) 前記シフト・レジスタの複数のビットによってアドレス指定される参照テーブルからの値；

から成る群から選択される入力に基づくことを特徴とする請求項 9 記載の方法。

【発明の詳細な説明】

選択可能なタップを備えたフィードバック・レジスタを
有する暗号化装置およびその方法

発明の分野

本発明は通信システムに関し、更に特定すれば、暗号化変数としてフィードバック・レジスタ出力を用いる通信システムにおける暗号化に関するものである。このフィードバック・レジスタは、暗号に対する攻撃 (cryptographic attack) から通信システムを保護するための選択可能なタップを含む。

発明の背景

多くの通信システムは、現在システムの機密保持を強化するために暗号を用いている。これら通信システムには、セルラ無線電話通信システム、個人通信システム、ページング・システム、ならびに有線および無線データ・ネットワークが含まれるが、これらに限定される訳ではない。以下一例として、セルラ通信システムについて述べる。しかしながら、ここで述べる暗号化技術は、本発明の範囲および精神から逸脱することなく、他の通信システムにも容

易に拡張可能であることは、当業者には認められよう。

ここでセルラ通信システムに移る。これらのシステムは、典型的に、無線周波数 (RF) 通信リンクを通じて固定ネットワーク装置 (即ち基地局) と交信する加入者装置 (移動機または携帯装置等) を含む。セルラ通信システムでは、RF 通信リンクが無許可の情報侵入 (スプーフィング (spoofing)) や情報抜取 (盗聴 (eavesdropping)) を最も受け易いので、これが暗号システムの主要な目標となっている。これらの通信リンクにおける情報は、性質が疑似ランダムな疑似ノイズ (PN) で情報を暗号化することによって暗号的に保護していることは、当技術では公知である。例えば、送信の前に、情報信号と PN 信号との排他的論理和演算を行うことによって、暗号化を達成することができる。後に、受信プロセスにおいて、逆演算を行えばよい。

PN 信号は完全にランダムではないか、大まかな見れば (cursory inspection) ランダムであるように思われる。これら PN 信号の利点は、線形フィードバッ

ク・シフト・レジスタ (LFSR) によって容易に発生できることである。LFSRは周期的な (即ち、決定論的な (deterministic)) PN信号を発生する。PN信号の周期性は、レジスタ内の段数 (即ち、記憶されるビット)、フィードバック・タップ、およびLFSR段の初期状態に依存する。LFSRは、多項式の各係数について、1つのフィードバック信

号「タップ」 (段の出力ビット) を有することによって、N次多項式を実施する (ここで、NはLFSRの段数)。入力ビットは、これらフィードバック信号タップの出力に対する排他的論理和演算と、レジスタへのフィードバックとによって形成される。理想的なのは、フィードバック「タップ」は、最大長PN信号発生器を実施するように選択できることである。最大長PN発生器は、 $2^N - 1$ 周期毎に繰り返す疑似ランダム・シーケンスを発生する。ここでNはレジスタ内の段数である。いくつかの異なる段数を有するレジスタの最大長フィードバック・タップ構成か、W. Wesley PetersonおよびE. J. Weldon, Jr. による "Error-Correcting Codes", second edition, MIT Press, 1972に記載されている。

PNレジスタを用いて情報信号を暗号的に保護する際の問題点は、それらが非常に攻撃を受けやすいことである (即ち、暗号化を解読する (crack) 即ち見破る (break) のが容易である)。LFSRに基づくPN発生器の弱点は、第一に発生器の固有な線形性によるものである。PN発生器はあるアルゴリズムにしたがって動作するので、そのアルゴリズムの知識によってシーケンス全体が判明されてしまう。更に、"Cipher Systems" by Henry Baker and Fred Piper, Northwood Publications, 1992の章に注記されているように、暗号分析は、N段のLFSRについて、 $2N$ ビットの平文 (plaintext) と対応する暗号

文 (ciphertext) についてのみ行えば、フィードバック「タップ」、LFSRの初期状態、そして究極的にLFSRによって出力されるいかなるPN信号出力も判定することができる。この攻撃容易性 (vulnerability) は、通信システムを暗号によって保護するためにLFSRを連続使用することに対する重大な欠点を意味する。

したがって、これらの問題を軽減することができる、通信システム用暗号化保護技術が必要とされている。

発明の概要

疑似ランダム・ビット・シーケンスを発生する方法および装置が提供される。第 1 フィードバック・アルゴリズムにしたがって、第 1 入力ビットがシフト・レジスタ内に記憶されるビットの関数として決定される。更に、第 2 フィードバック・アルゴリズムにしたがって、第 2 入力ビットが前記シフト・レジスタ内に記憶されるビットの関数として決定される。続いて、前記シフト・レジスタによって非線形疑似ランダム・シーケンスが生成されるように、前記シフト・レジスタに供給される特定の入力ビットが、前記第 1 入力ビットおよび第 2 入力ビットから成る群から決定論的に (deterministically) 選択される。更に、前記疑似ランダム・ビット・シーケンスを利用して送信すべき信号を暗号化すると共に受信信号を復号化する通信装置について

ても記載する。

図面の簡単な説明

第 1 図は、本発明による、加入者装置と固定ネットワーク通信装置とを有する通信システムにおいて用いられる、好適実施例の暗号化プロセスを示すブロック図である。

第 2 図は、本発明による、第 1 図に示された加入者装置または固定ネットワーク通信装置のいずれかによって用いられる、好適実施例の疑似ランダム・ビット・シーケンス発生器のブロック図である。

好適実施例の詳細な説明

ここで第 1 図を参照して、本発明による加入者通信装置 202 と固定ネットワーク通信装置 200 (即ち、セルラ基地局) とを有する通信システムにおいて用いられる、好適実施例の暗号化プロセスを示す。固定ネットワーク通信装置 200 は、カプラ 212 によって基地局制御器 210 を通じて、固定ネットワークの他の部分に接続されている。固定ネットワークの他の部分には、他の通信装置、中央制御部、通信システム交換機、または公衆電話交換網 (PSTN) 上のアク

セス・ポートを含むが、これらに限定される訳ではない。動作中、固定ネットワークから（カプラ2

12を通じて）または加入者通信装置202の他の部分から、情報信号（即ち、音声および／またはデータ信号）が通信システムに入力される。続いて、前記情報信号は暗号化されて通信チャンネル204を通じて送信され、更にその情報信号を送信しなかった通信装置（即ち、それぞれ固定ネットワーク通信装置200または加入者通信装置202のいずれか）によって受信され復号化（decrypt）される。

一例として、固定ネットワーク通信装置200から加入者通信装置202への情報信号の通信について以下に述べる。情報信号212は、固定ネットワーク通信装置200の基地局制御器210に入力される。基地局制御器210は、暗号化保護を行う以外にも、情報信号212の通信に関連するいくつかの他の動作を行うこともできる。これら他の動作には、エラー保護符号化、音声符号化（ボコーティング）、チャンネル・コード化、変調、および信号出力増幅が含まれるが、これらに限定されるわけではない。しかしながら、これら他の動作は、当技術ではよく知られている多くの異なる方法で行うことができる。本発明の好適実施例による暗号化保護方式に特定して焦点を当てることができるように、かかる他の動作について以下の説明ではこれ以上論じないことにする。

一旦情報信号212が基地局制御器210に入力されると、この情報信号は暗号化される。好ましくは、この暗号化は、入来する情報信号212、224を排他的論理和

（XOR）ゲート226に供給し、PN発生器222からの疑似ランダム信号218とそれを組み合わせることによって行う。好適実施例では、疑似ランダム信号218は非線形信号である。この非線形疑似ランダム信号218を発生する方法については、第2図を参照して後に論じる。XORゲート226の出力228は、暗号化情報信号である。この暗号化情報信号228は、信号送信線を通じてアンテナ206に結合されその後無線通信チャンネル204を通じて送信される

のに先だって、基地局制御器210によって更に処理することもできる。本発明の範囲および精神から逸脱することなく、入来情報信号224を他の関数（即ちXOR関数以外のもの）にしたがって組み合わせてもよいことを、当業者は認めよう。

加入者装置202は、アンテナおよび信号送信線208によって暗号化情報信号を受信する。受信された暗号化情報信号208, 234はXORゲート236に入力され、PN発生器242からの疑似ランダム信号238と組み合わせられて、情報信号が復号化される。PN発生器242はPN発生器222と同期され、双方のPN発生器によって出力されるPN信号218, 238が暗号化情報信号と同期するようにしなければならないことは認められよう。PN信号238が受信された暗号化情報信号234と適正に同期されているとき、XORゲート236の出力240は復号化された情報信号となる。この復号化情報信号240

は、情報信号250として加入者装置から出力されるのに先だって、加入者装置202によって更に処理を行うことができる。

同様に、加入者通信装置202から固定ネットワーク通信装置200に情報信号を通信することもできる。情報信号250は加入者装置202に入力される。入来する情報信号250, 244は、XORゲート246によって、非線形疑似ランダム信号238を用いて暗号化される。XORゲート246の暗号化情報信号出力248は、通信線上のアンテナ208に結合され、無線通信チャンネル204上を送信される。固定ネットワーク通信装置200は、暗号化情報信号206を受信し、それを基地局制御器210に供給する。基地局制御器210は、XORゲート216によって受信した暗号化情報信号206, 214を非線形疑似ランダム信号218と結合し、情報信号を復号化する。非線形疑似ランダム信号218は、情報信号を暗号化するために当初用いられた非線形疑似ランダム信号238と同期されている。XORゲート216は、復号化された情報信号220を出力し、次に情報信号220はカプラ212を通じて固定ネットワークに供給される。

次に第2図を参照すると、加入者装置202または固定ネットワーク通信装置

200のいずれかによって用いられる、好適実施例の疑似ランダム信号（即ち、ビット・シーケンス）発生器222のブロック図が示されている。一例

として、7ビットの疑似ランダム・ビット・シーケンス発生器222、242について説明する。しかしながら、これよりも大きな疑似ランダム・ビット・シーケンス発生器を用いて情報信号を暗号化し、情報信号の暗号化保護を更に改良可能であることは、当業者には認められよう（即ち、長い非線形疑似ランダム・ビット・シーケンスは短いものよりも、「見破る」即ち「解読する」のが困難である）。加えて、かかる長い疑似ランダムビット・シーケンス発生器を用いることは、本発明の範囲および精神から逸脱することではない。

好ましくは、7ビット疑似ランダム・ビット・シーケンス発生器222、242は、いくつかの多項式関数（polynomial function）を実施するフィードバック・レジスタとして、そして所定ビット数（例えば、 $D_0 \sim D_6$ まで付番された7ビット）を記憶するためのシフト・レジスタ252を含むものとして実施される。加えて、第1フィードバック回路254がシフトレジスタ252に動作可能に結合されている。好適実施例では、第1フィードバック回路は、シフト・レジスタ252内に記憶されているビットから、XORゲート254への入力（即ち、 D_3 、 D_6 ）を「抜き取る（tapping）」ことによって、多項式関数 $x^7 + x^3 + 1$ を実行する。XORゲート254の出力は第1入力ビット260を決定し、これをシフト・レジスタ252の直列入力に選択的に入力することができる。第2フィードバック

回路256もシフト・レジスタ252に動作可能に結合されている。好ましくは、第2フィードバック回路は、シフト・レジスタ252内に記憶されているビットから、XORゲート254への入力（即ち、 D_2 、 D_3 、 D_4 、 D_6 ）を「抜き取る」ことによって、多項式関数 $x^7 + x^4 + x^3 + x^2 + 1$ を実行する。XORゲート256の出力は、第2入力ビット262を決定し、これをシフト・レジスタ252の直列入力に選択的に入力することができる。第1および第2入力ビット260、262はフィードバック選択制御器266に入力され、2つの入力ビット

の一方がシフト・レジスタ252に出力される(268)。フィードバック選択制御器266は、あるアルゴリズムにしたがって、シフト・レジスタ252および直列出力218, 238上の出力によって、非線形疑似ランダム・シーケンスが生成されるように、シフト・レジスタ252に供給すべき特定の入力ビット(即ち、入力ビット260または262のいずれか)を決定論的に選択する。疑似ランダム・シーケンスが出力218, 238となることを保証するために、疑似ランダム・ビット・シーケンス発生器222, 242を初期化し数サイクルの間クロック駆動して、出力シーケンスがランダムに混合されるようにする必要がある。疑似ランダム混合に必要な最少クロック・サイクル数はNであり、このNはシフト・レジスタ252の長さである(この例では7クロック・サイクルが必要となる)。加えて、暗号攻

撃(即ち、暗号解読)を被る可能性(susceptibility)を防ぐために、フィードバック選択制御器266は、2Nクロック・サイクル以上の間、同じフィードバック回路254または256から特定の入力ビットを選択してはならない。ここで、Nはシフト・レジスタ252の長さである。異なるフィードバック回路から入力ビットを選択する頻度を高めることによって、暗号攻撃者が線形式解法攻撃(linear equation solution attack)を使用できないようにする。最後に、シフト・レジスタ252に直列的に入力される疑似ランダム・シーケンス268の非線形性を高めるためには、2つ以上のフィードバック回路を用いればよいことは、当業者には認められよう。

好ましくは、フィードバック選択制御器266は、内部制御機構を含み、これが内部入力264に基づくアルゴリズムにしたがって特定の入力ビットを選択する(即ち、それらの間で切り替える)。内部入力264は、シフト・レジスタ252の複数の「抜き取られていない(untapped)」ビット(例えば、D₀, D₁, のANDゲート機能)のゲート機能258の出力で構成される。この内部制御機構がこのアルゴリズムにしたがって動作する場合、シフトレジスタに連続的に供給される入力ビットは、以下の表1に示す通りである。

表 1

レジスタ段	制御ビット	切り替え	新入力ビット
1 0 1 0 1 0 1	$1 \cdot 0 = 0$	アップ	$0 \oplus 1 = 1$
1 1 0 1 0 1 0	$1 \cdot 1 = 1$	ダウン	$0 \oplus 1 \oplus 0 \oplus 0 = 1$
1 1 1 0 1 0 1	$1 \cdot 1 = 1$	アップ	$0 \oplus 1 = 1$
1 1 1 1 0 1 0	$1 \cdot 1 = 1$	ダウン	$1 \oplus 1 \oplus 0 \oplus 0 = 0$
0 1 1 1 1 0 1	$0 \cdot 1 = 0$	ダウン	$1 \oplus 1 \oplus 1 \oplus 1 = 0$
0 0 1 1 1 1 0	$0 \cdot 0 = 0$	ダウン	$1 \oplus 1 \oplus 1 \oplus 0 = 1$
1 0 0 1 1 1 1	$1 \cdot 0 = 0$	ダウン	$0 \oplus 1 \oplus 1 \oplus 1 = 1$
1 1 0 0 1 1 1	$1 \cdot 1 = 1$	アップ	$0 \oplus 1 = 1$
1 1 1 0 0 1 1	$1 \cdot 1 = 1$	ダウン	$1 \oplus 0 \oplus 0 \oplus 1 = 0$
0 1 1 1 0 0 1	$0 \cdot 1 = 0$	ダウン	$1 \oplus 1 \oplus 0 \oplus 1 = 1$
.	.	.	.
.	.	.	.
.	.	.	.

他の内部制御機構を用いてもよいことは認められよう（例えば、シフト・レジスタ 252 のパリティ・ビットまたはシフト・レジスタ 252 の複数のいずれかのビット（即ち、「抜き取られた」または「抜き取られていない」）の関数）。加えて、フィードバック選択制御器 266 は、外部入力に基づくアルゴリズムにしたがって特定の入力ビットを選択する外部制御機構を含んでもよい。外部入力の

例は、線形フィードバック・シフト・レジスタ出力、クロック初期化信号、およびセルラ・オートマトン（cellular automaton）を含む。セルラ・オートマトンの概念は、1990 International Test Conferenceで紹介された論文の中の、Paul H. Bardell による “Analysis of Cellular Automata Used as Pseudorandom Pattern Generators” において論じられている。更に、フィードバック選択制御器

266は、内部および外部制御機構の組み合わせを含むこともできる。最後に、フィードバック選択制御器266は、シフト・レジスタ252の複数のビットによってアドレス指定される参照テーブルから値を選択することによって、特定の入力ビットを選択するという、全く異なる制御機構を用いることもできる。

本発明の好適実施例は、加入者通信装置202を参照して以下のように要約することができる。供給元通信システム(serving communication system)の加入者装置202と固定ネットワーク通信装置200との間で、暗号化プロセスによって機密保持通信を維持するために用いられる通信装置が提供される。前記通信装置の送信部は、非線形疑似ランダム・ビット・シーケンス238を発生する、疑似ランダム・ビット・シーケンス発生器242を含む。前記疑似ランダム・ビット・シーケンス発生器242は、所定数のビット(即ち、D₀~D₆)を記憶するためのシフト・レジスタ252を含む。更に、第1フィードバック装

置254が前記シフト・レジスタ252に動作可能に結合されている。前記第1フィードバック装置254は、前記シフト・レジスタ252に記憶されているビットの関数として、第1入力ビット260を決定する。更に、第2フィードバック装置256が前記シフト・レジスタ252に動作的に結合されている。前記第2フィードバック装置256は、前記シフト・レジスタ252に記憶されているビットの関数として、第2入力ビット262を決定する。最後に、前記疑似ランダム・ビット・シーケンス発生器242は、前記シフト・レジスタ252、第1フィードバック装置254、および第2フィードバック装置256に動作可能に結合された制御器266を含む。この制御器266は、前記シフト・レジスタ252に供給すべき特定入力ビット268を決定論的に選択する。この特定入力ビットは、前記第1入力ビット260または第2入力ビット262のいずれかである。

前記通信装置の送信部は、前記疑似ランダム・ビット・シーケンス発生器242に動作的に結合されている暗号化装置246も含む。これは、前記非線形疑似ランダム・ビット・シーケンス238の関数として、入力情報信号244、250を暗号化する。送信機208が前記暗号化装置246に動作可能に結合され、

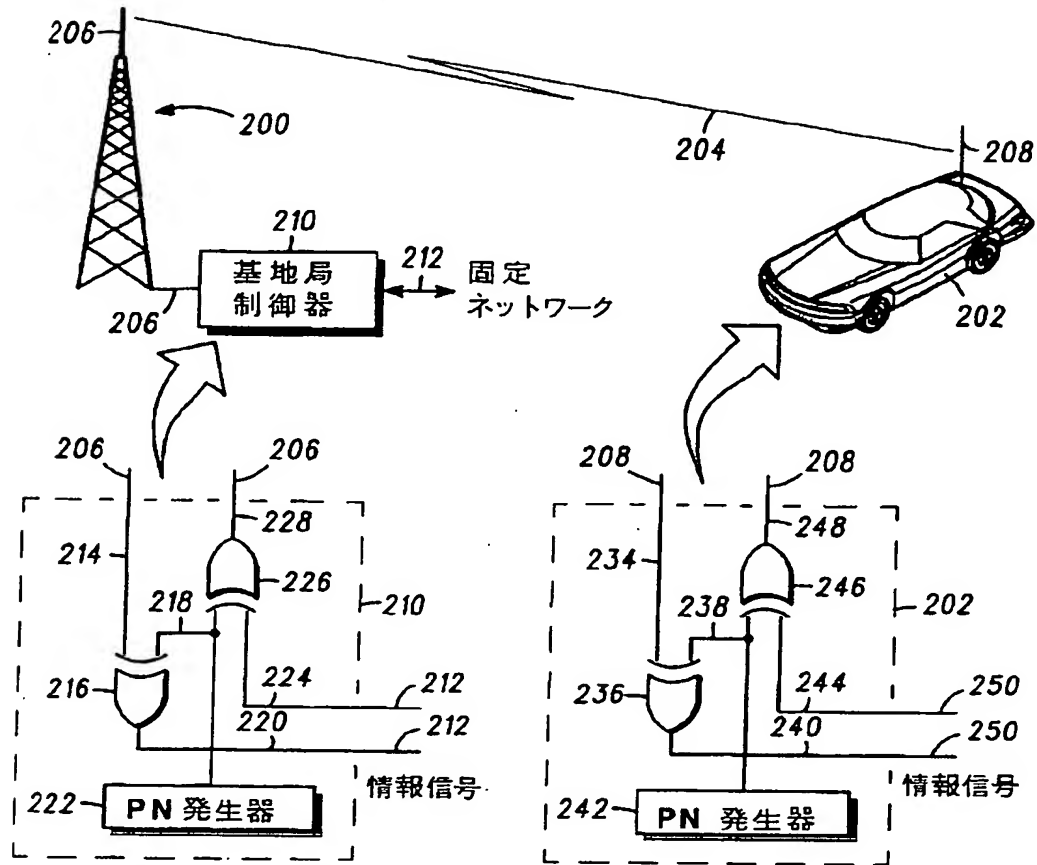
通信チャンネル 204 を通じて前記暗号化された情報信号 248 を送信する。

前記通信装置の受信部は、通信チャンネル 204 から暗

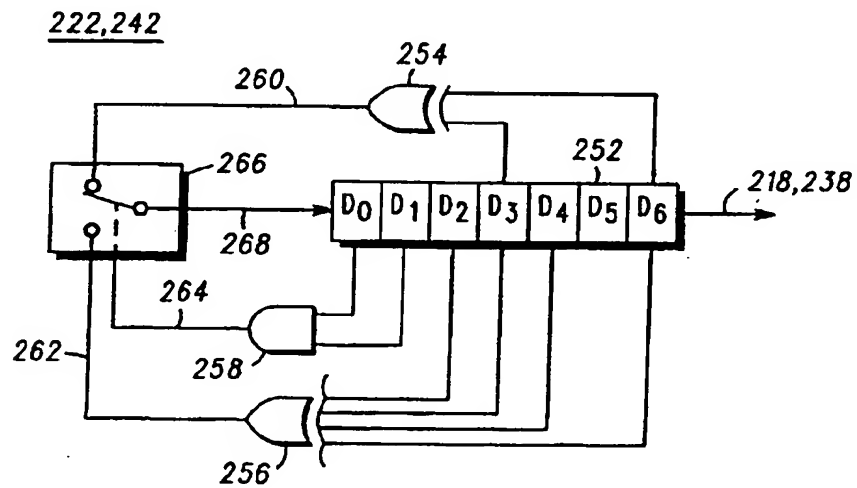
号化情報信号を受信する受信機 208 を含む。更に、前記受信部は、前記送信部が用いたのと同じまたは少なくとも実質的に同様の疑似ランダム・ビット・シーケンス発生器 242 を用いる。この疑似ランダム・ビット・シーケンス発生器 238 は、非線形疑似ランダム・ビット・シーケンス 238 を発生する。最後に、復号化装置 236 が前記受信機 208 および疑似ランダム・ビット・シーケンス発生器 238 に動作的に結合され、前記非線形疑似ランダム・ビット・シーケンス 238 の関数として、受信した暗号化情報信号を情報信号 240, 250 に復号化する。

以上、本発明をある程度特定して記載しかつ図示したが、本実施例の開示は例として行われたに過ぎず、部分および工程の構成および組み合わせにおいて多数の変更が、主張される本発明の精神および範囲から逸脱することなく、当業者には想起されよう。例えば、代替的に、通信チャンネルは、電子データ・バス、有線、光ファイバ・リンク、衛星リンク、または他のいずれのタイプの通信チャンネルに置き換えることができる。

【図1】




【図2】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US94/07774

A. CLASSIFICATION OF SUBJECT MATTER IPC(5) : G06F 1/02 US CL : 380/46 According to International Patent Classification (IPC) or to both national classification and IPC				
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) U.S. : 380/46 380/9, 49, 50: 331/78: 364/717 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)				
C. DOCUMENTS CONSIDERED TO BE RELEVANT				
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.		
A	US, A, 3,728,533 (MATTHEWS) 17 APRIL 1973.	1-10		
A	US, A, 4,590,601 (BEEMAN) 20 MAY 1986.	1-10		
A	US, A, 4,611,183 (PIOSENKA ET AL) 08 SEPTEMBER 1986.	1-10		
A	US, A, 4,890,252 (WANG) 26 DECEMBER 1989.	1-10		
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.				
<table border="0"> <tr> <td> * Special categories of cited documents: "A" document defining the general state of the art which is not considered to be part of particular relevance "E" earlier documents published on or after the international filing date "F" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "G" document referring to an oral disclosure, use, exhibition or other means "H" documents published prior to the international filing date but later than the priority date claimed </td> <td> "I" later documents published after the international filing date or priority date and not in conflict with the application but cited to underlain the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" documents of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "Z" document member of the same patent family </td> </tr> </table>			* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be part of particular relevance "E" earlier documents published on or after the international filing date "F" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "G" document referring to an oral disclosure, use, exhibition or other means "H" documents published prior to the international filing date but later than the priority date claimed	"I" later documents published after the international filing date or priority date and not in conflict with the application but cited to underlain the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" documents of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "Z" document member of the same patent family
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be part of particular relevance "E" earlier documents published on or after the international filing date "F" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "G" document referring to an oral disclosure, use, exhibition or other means "H" documents published prior to the international filing date but later than the priority date claimed	"I" later documents published after the international filing date or priority date and not in conflict with the application but cited to underlain the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" documents of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "Z" document member of the same patent family			
Date of the actual completion of the international search 25 AUGUST 1994		Date of mailing of the international search report SEP 02 1994		
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230		Authorized officer  BENJAMIN EARL GREGORY Telephone No. (703) 308-0479		

フロントページの続き

(51) Int. Cl. 6	識別記号	庁内整理番号	F I
H O 4 K 1/06		8842-5 J	
H O 4 L 9/00			
H O 4 Q 7/38			